



CompTIA SOT-001

CompTIA SecOT+ (V1)

Thank You for Downloading SOT-001 Updated Exam Questions

<https://certs4sale.com/comptia/sot-001-pdf-exam-dumps>

Question: 1

A Security Operations Center (SOC) primarily exists to:

- A. Develop new software applications
- B. Monitor, detect, and respond to security threats
- C. Manage corporate finance systems
- D. Perform marketing analytics

Answer: B

Explanation:

A SOC focuses on continuous monitoring, threat detection, and incident response to protect organizational assets. It acts as the central hub for security operations and response activities.

Question: 2

A Tier 1 SOC analyst is mainly responsible for:

- A. Threat hunting and malware reverse engineering
- B. Initial alert triage and escalation
- C. Developing security policies
- D. Performing forensic investigations

Answer: B

Explanation:

Tier 1 analysts handle initial alert review, validation, and escalation to higher tiers if required. They focus on monitoring dashboards and identifying false positives.

Question: 3

The MITRE ATT&CK framework is best described as:

- A. A vulnerability scoring system
- B. A compliance auditing framework
- C. A knowledge base of adversary tactics and techniques
- D. A penetration testing tool

Answer: C

Explanation:

MITRE ATT&CK documents real-world adversary behaviors and maps tactics and techniques used during cyber attacks. It helps SOC teams improve detection and response.

Question: 4

Which phase of the attack lifecycle involves gaining initial access?

- A. Command and control

- B. Reconnaissance
- C. Delivery and exploitation
- D. Exfiltration

Answer: C

Explanation:

Delivery and exploitation is the phase where attackers deliver payloads and exploit vulnerabilities to gain access to systems.

Question: 5

Which threat uses trusted system tools to avoid detection?

- A. Ransomware
- B. Fileless malware
- C. Boot sector virus
- D. Macro virus

Answer: B

Explanation:

Fileless malware leverages legitimate system tools and memory execution, making it harder to detect using traditional antivirus solutions.

THANK YOU FOR DOWNLOADING SOT-001 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our SOT-001 Exam Product

Visit Our Site to Purchase the Full Set of Actual SOT-001 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/comptia/sot-001-pdf-exam-dumps>